Wilmington Police Department

Directive: .06.09

Automated License Plate Readers

CALEA Standards: 41.3.9

I. Purpose:

This directive establishes procedures and guidelines for the use and oversight of the department's fixed and mobile Automated Licenses Plate Reader (ALPR) technology.

II. Definitions:

A. Automated License Plate Reader (ALPR) – A device that uses cameras and computer technology to compare digital images of license plates to lists of known plates of interest. ALPR's may be deployed in different configurations including fixed and mobile cameras. Both configurations operate in the same manner for the same purpose.

1. Fixed ALPR locations use cameras that are engineered to focus on the rear license plate of vehicles passing by the camera location. The camera image is sent by cellular data signal to an off-site server where the image is compared with license plates entered into the National Crime Information Center (NCIC) and hot lists as defined below. Only license plates that match an NCIC entry or hot list entry will trigger an alert. The images of the license plates of the vehicles passing by the camera are retained for no longer than 60 days.

2. Mobile ALPR systems work in the same manner. The cameras may be mounted on a vehicle or on a mobile trailer. The ALPR users who are logged in to monitor that particular camera will receive an alert if a captured image matches an NCIC entry or hot list entry.

B. Hot List – A license plate associated with a vehicle of interest from NCIC or a vehicle involved in a criminal investigation.

C. Scan File Data – Information obtained by an ALPR of license plates within public view that were read by the device, including images of the plate and vehicle on which it was displayed, and information regarding the location of the police cruiser or stationary camera position at the time the information was captured. Information stored includes a photo of the registration plate showing the rear of the vehicle, a date and time stamp of when the registration plate was read by the ALPR and a GPS coordinate to identify the location the registration plate was read by the ALPR.

III. Procedure:

A. Overview

1. The ALPR works by comparing hot list data with the scan file. The device will alert the user of potential matches. The user must take steps to validate the alert itself. Officers should be mindful that the ALPR may produce erroneous alerts due to damaged license plates, system misread, misidentification of a plate state, or the variety of license plate types, etc.

2. Any traffic stops based on the alert from the ALPR must comply with all laws and procedures for a traffic stop.

3. Upon receiving an ALPR alert generated from a NCIC file, officers must confirm the status of the NCIC hit prior to taking any enforcement action.

4. If the ALPR alert is from a custom hot list, officers will follow the instructions in the reason code of the notification. If there are no instructions in the reason code, or if the NCIC hit cannot be verified, officers will need to develop reasonable suspicion independently of the ALPR alert prior to taking enforcement action.

5. There may be alerts that will not always require action, such as NCIC Nationwide Domestic Violence Protection Orders.

B. Development of the Hot List

1. Information will be submitted to Axon Enterprise in the following ways:

   a. Available NCIC extract downloads occur twice daily and will transfer that hot list data to the ALPR server.

   b. Authorized users of the ALPR during their shift may only enter additional vehicles of interest to the hot list for official and legitimate law enforcement purposes with prior supervisory approval.

   c. Other local hot lists may be developed for manual entries through the current ALPR system.

2. Hot lists will primarily be compiled from vehicles associated with NCIC entries for the following categories:

   a. Stolen Vehicles
   b. Gang or Suspected Terrorists
   c. Missing Persons
   d. Stolen License Plates
   e. Wanted Persons with Warrants Entered into NCIC

3. Hot lists may also include vehicles from any of the following categories:

   a. Homicides
   b. Aggravated Assaults/Sexual Assaults
   c. Robbery
   d. Kidnapping
   e. Burglary or Break-In
   f. Amber Alert/Silver Alert/Blue Alert etc.
   g. Involuntary Commitment Orders/Mental patient currently in crisis
   h. Stolen Property
   i. Hit and Run Vehicle
   j. Vehicle that fled from a traffic stop
   k. Requests for assistance from other agencies
   l. Narcotics investigations
   m. Investigations approved by the officer's supervisor

4. Hot lists **shall not** include license plates associated with regulatory motor vehicle violations (i.e. expired registration, inspection violations, drivers license violations).

C. Usage/Limitations/Security

1. Only authorized personnel trained in the use of ALPR shall operate the system. All authorized personnel will complete the required training.

2. Scan file data will, on an ongoing basis, be automatically uploaded from the ALPR in the car to the ALPR server. On fixed cameras, all lists will update automatically.

3. Department personnel are responsible for the security of the ALPR data and may only access, use, release and/or disseminate hot list and scan file data for official and legitimate law enforcement purposes:

   a. As with other similar data, the department will ensure that the storage, use and transmission of scan file and hot list data is as secure as reasonably possible. Access to both shall be restricted only to sworn law enforcement personnel and designated non-sworn personnel.

   b. Hot list data will be considered confidential information. Security of the hot list data will be the responsibility of the officer using the ALPR or personnel accessing the data.

   c. Scan file data will be considered confidential information. Access to scan files will be secured and controlled by a login/password accessible system, capable of documenting who accessed the information by identity, date and time. Officers may only access data stored in the ALPR server based upon a reasonable belief that the scan file data may be related or useful as part of a specific official action or investigation.

d. This section also applies to shared data obtained by ALPR systems not operated by this agency.

4. The STING Center is responsible for the approval of hot lists by officers. STING Center personnel are to ensure that the reason code for hot lists include information as to:

   a. Why the vehicle is of interest,
   b. What action, if any, other officers should take if the vehicle is located,
   c. Who is to be contacted after the vehicle is located, and
   d. If a case number is associated with a vehicle, the case number is to be included in the hot list entry.

5. The on-duty Watch Commander may approve requests from other surrounding law enforcement agencies without ALPR capabilities for use of the ALPR, as the situation and resources allow.

6. WPD officers may retain ALPR data beyond 60 days for criminal investigative reasons only. If the data need to be maintained beyond 60 days, a copy of the information should be acquired and placed into the case management system and documented via the investigative report or a supplement report. The ALPR system automatically purges all stored data after 60 days.

D. Program Oversight/Evaluation/Audit Review

1. All requests for shared data access from other law enforcement agencies and/or invitations to access data from private ALPR systems (i.e. HOA's, Community Watch Groups) shall be forwarded to the Chief of Police for approval.

2. Damage or other malfunctions to the equipment will be reported to the officer's immediate supervisor.

3. All successful uses of the ALPR shall be documented and forwarded to the ALPR program supervisor.

4. The supervisor of the ALPR program will be responsible for conducting, reviewing and retaining audits of the ALPR system. These audits shall be forwarded through the chain of command to the Chief of Police annually. The audit information should include the following:

   a. Records of ALPR operators and their ALPR usage, including vehicles of interest added to a hot list by individual officers.

   b. A listing of access to the department's server, to include, additions and/or searches of the scan file, in order to verify security of that data and compliance with this policy.

   c. Auditing the local hot lists to ensure manual entries are being deleted when no longer of interest.

5. Anyone becoming aware of a possible violation of this policy, including but not limited to the unauthorized access, use, release and/or dissemination of ALPR data, shall refer the matter to their supervisor.